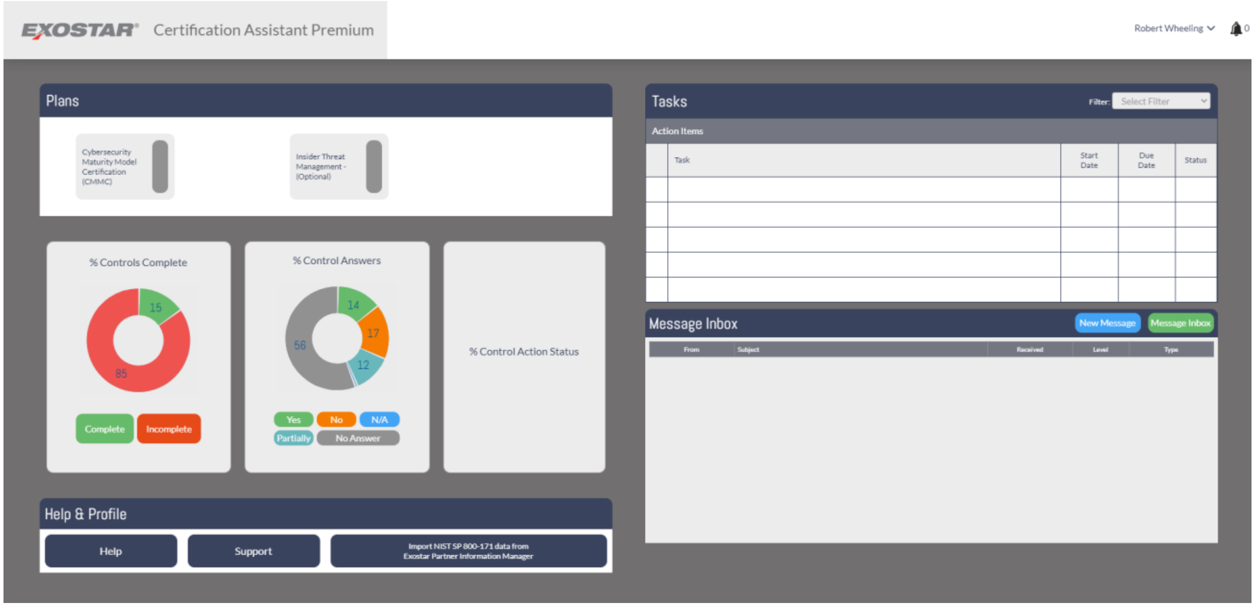
Insider Threat Management

Contents

Accessing Insider Threat Management

As part of the Certification Assistant Premium license, you now have access to an optional module called Insider Threat Management. The new module will appear in the Plans section on the home page, click to enter the module.



What is it and why do I need it?

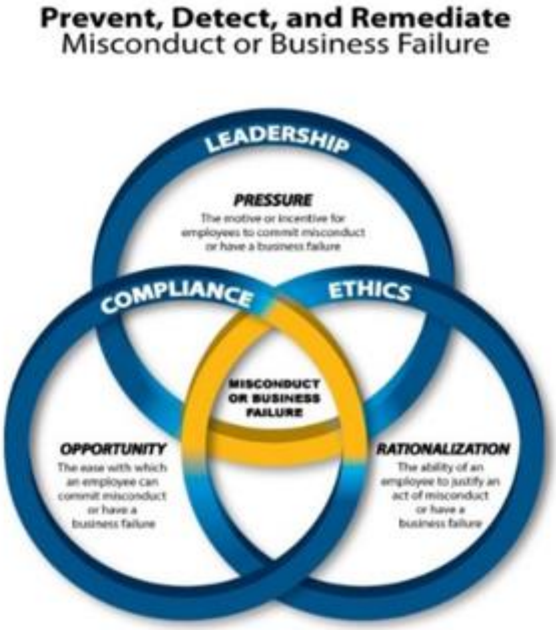
This module is provided as an option for companies wanting an understanding of not just the risk of a failed control, but the risk around human behavior (Fraud Triangle) that could cause a compliance failure. The risk assessment associated with this module may support but does not replace the risk assessment required for Cybersecurity Maturity Model Certification (CMMC).

The Fraud Triangle is a more versatile way to manage compliance risk. Compliance failure or misconduct always happens in three parts:

- First, an employee must feel compelled to take some act; that's *Pressure*
- He/she needs *Opportunity* to proceed with the mistaken or wrongful act
- The employee must somehow justify (either by deliberate choice, or accidental ignorance) doing something that he/she should not do; that's *Rationalization*

Once a compliance manager frames compliance risk that way, the steps to address weaknesses in a compliance program become much clearer:

- Catalog the possible causes of a compliance risk (bribery, data security, fraud, harassment, and more), and place them in relative proportion to each other.
- Identify the steps necessary to remediate that risk as warranted.
- Assign accountability to specific individuals for those remediation steps.
- Monitor progress toward that remediation, and re-assess the severity of the risk on a regular basis



Prevent, Detect, and Remediate
Misconduct or Business Failure

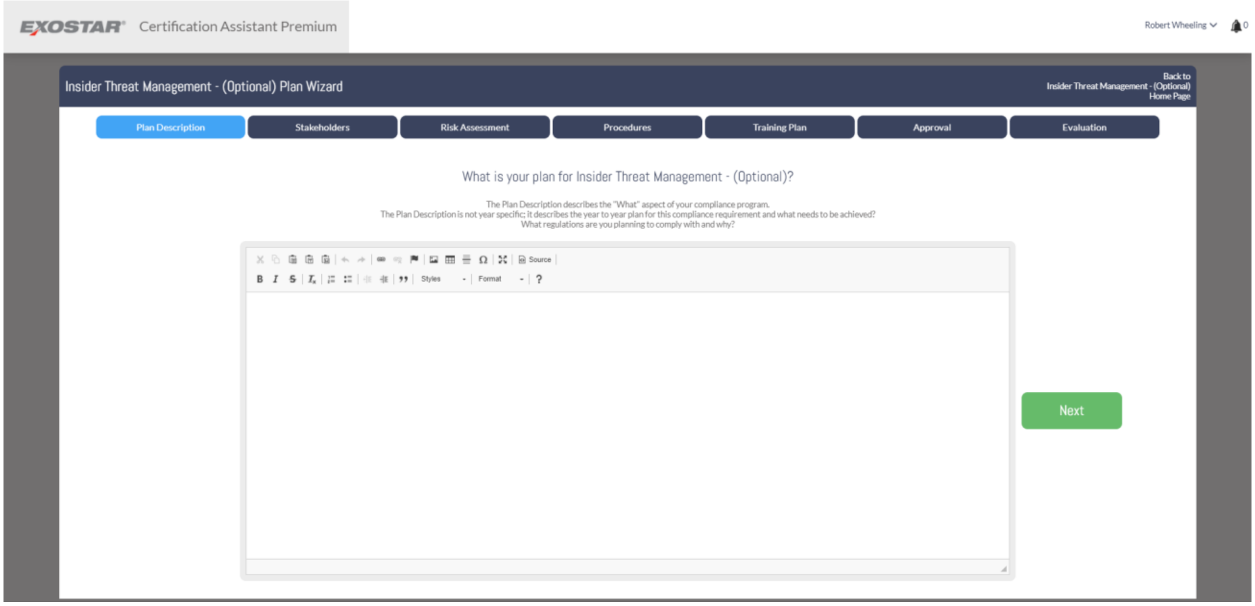
LEADERSHIP
PRESSURE
The motive or incentive for employees to commit misconduct or have a business failure
COMPLIANCE
ETHICS
MISCONDUCT OR BUSINESS FAILURE
OPPORTUNITY
The ease with which an employee can commit misconduct or have a business failure
RATIONALIZATION
The ability of an employee to justify an act of misconduct or have a business failure

Plan Description

The Plan Description describes the "What" aspect of your compliance program.

The Plan Description is not year specific; it describes the year to year plan for this compliance requirement and what needs to be achieved?

What regulations are you planning to comply with and why?



Insider Threat Management - (Optional) Plan Wizard

What is your plan for Insider Threat Management - (Optional)?

The Plan Description describes the "What" aspect of your compliance program.
The Plan Description is not year specific; it describes the year to year plan for this compliance requirement and what needs to be achieved?
What regulations are you planning to comply with and why?

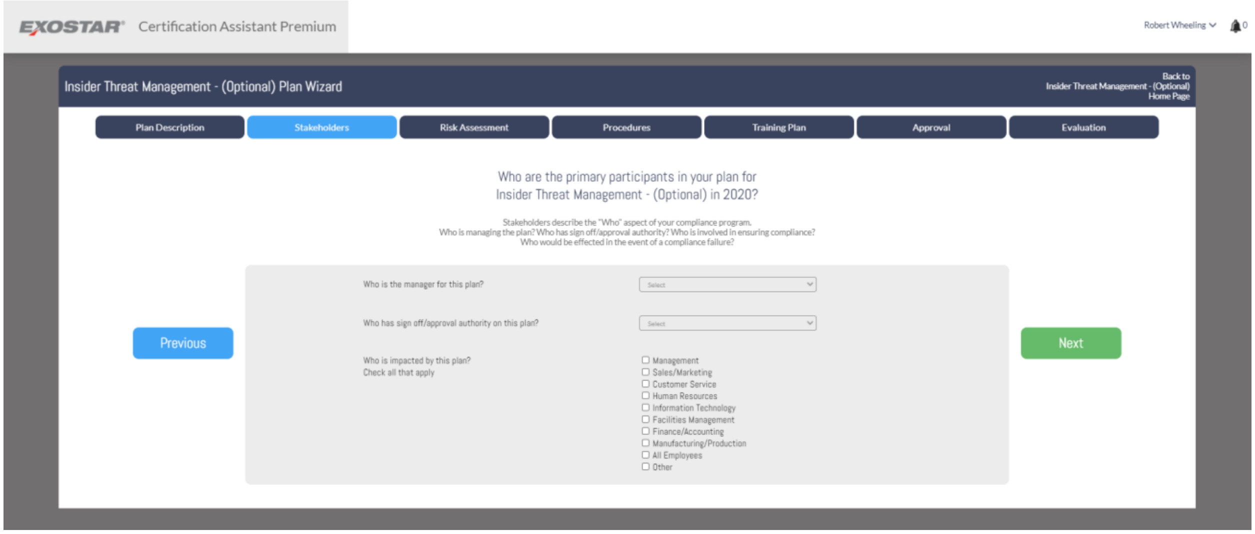
Enter your plan description narrative and click on the Next button to advance to the next section.

Stakeholders

Stakeholders describe the "Who" aspect of your compliance program.

Who is managing the plan? Who has sign off/approval authority? Who is involved in ensuring compliance?

Who would be affected in the event of a compliance failure?


EXOSTAR Certification Assistant Premium
Robert Wheeling
0
Insider Threat Management - (Optional) Plan Wizard
Back to Insider Threat Management - (Optional) Home Page
Plan Description
Stakeholders
Risk Assessment
Procedures
Training Plan
Approval
Evaluation
Previous
Next

Who are the primary participants in your plan for
Insider Threat Management - (Optional) in 2020?

Stakeholders describe the "Who" aspect of your compliance program.
Who is managing the plan? Who has sign off/approval authority? Who is involved in ensuring compliance?
Who would be effected in the event of a compliance failure?

Who is the manager for this plan? Select

Who has sign off/approval authority on this plan? Select

Who is impacted by this plan?
Check all that apply

□ Management
□ Sales/Marketing
□ Customer Service
□ Human Resources
□ Information Technology
□ Facilities Management
□ Finance/Accounting
□ Manufacturing/Production
□ All Employees
□ Other

Select the manager for the plan using the dropdown list of users in your account. Select the user with sign off/approval authority on the plan from the dropdown list. Check the departments that may be impacted by this plan from the generic list provided.

Use the Next or Previous buttons to move between sections.

Risk Assessment

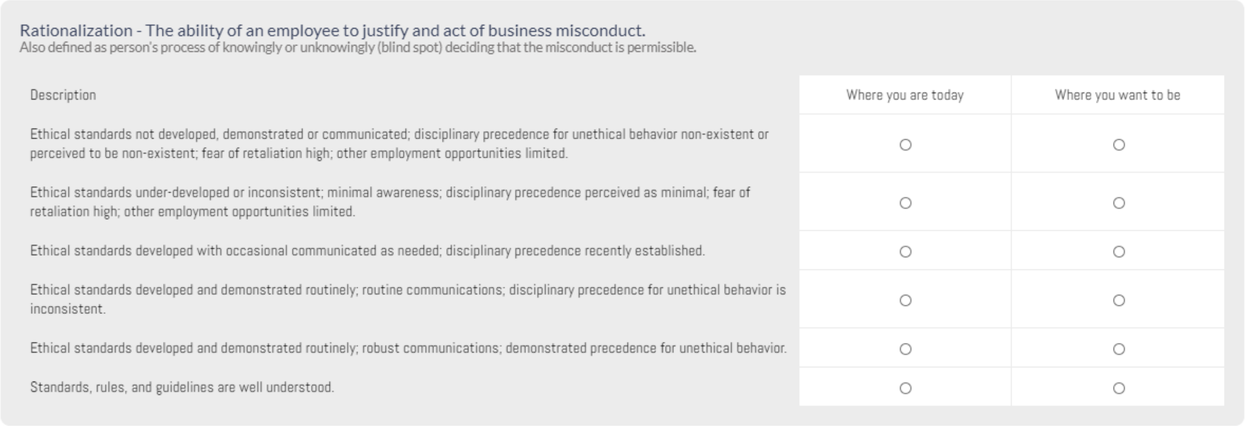
Where do you assess the current levels of your compliance program regarding Insider Threat Management and what sort of improvement would you like to see over the year?

It is always a good idea to determine where you currently are and get an idea of where you would like to be. Each of the following 4 questions will focus on compliance and ethics regarding this plan. Answer honestly and use this assessment to focus your efforts on achieving your improvement goals.

Rationalization

The ability of an employee to justify and act of business misconduct. Also defined as person's process of knowingly or unknowingly (blind spot) deciding that the misconduct is permissible.

In the tables below, select where your organization is today and where you would like to be by the end of the year.

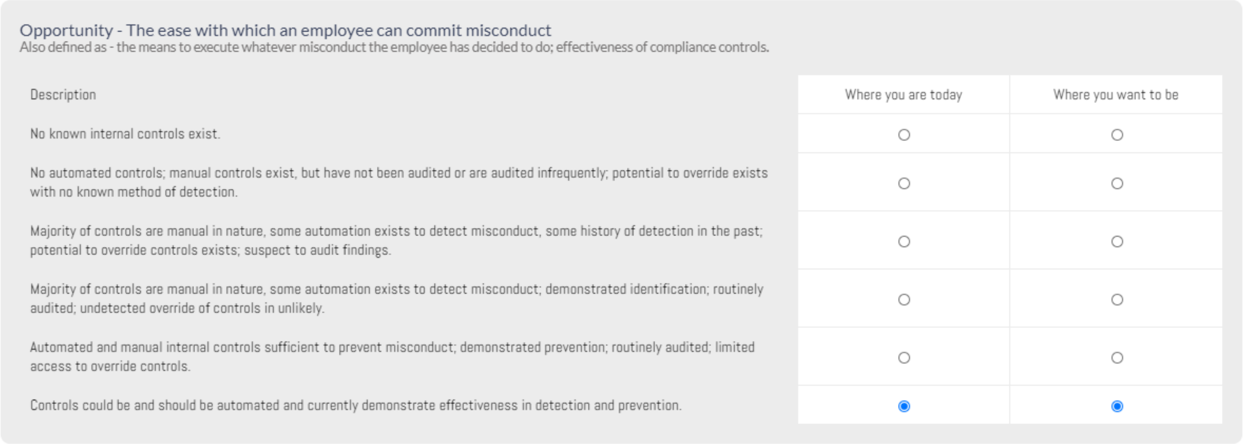


Rationalization - The ability of an employee to justify and act of business misconduct.
Also defined as person's process of knowingly or unknowingly (blind spot) deciding that the misconduct is permissible.

Description	Where you are today	Where you want to be
Ethical standards not developed, demonstrated or communicated; disciplinary precedence for unethical behavior non-existent or perceived to be non-existent; fear of retaliation high; other employment opportunities limited.	○	○
Ethical standards under-developed or inconsistent; minimal awareness; disciplinary precedence perceived as minimal; fear of retaliation high; other employment opportunities limited.	○	○
Ethical standards developed with occasional communicated as needed; disciplinary precedence recently established.	○	○
Ethical standards developed and demonstrated routinely; routine communications; disciplinary precedence for unethical behavior is inconsistent.	○	○
Ethical standards developed and demonstrated routinely; robust communications; demonstrated precedence for unethical behavior.	○	○
Standards, rules, and guidelines are well understood.	○	○

Opportunity

The ease with which an employee can commit misconduct. Also defined as - the means to execute whatever misconduct the employee has decided to do, effectiveness of compliance controls.

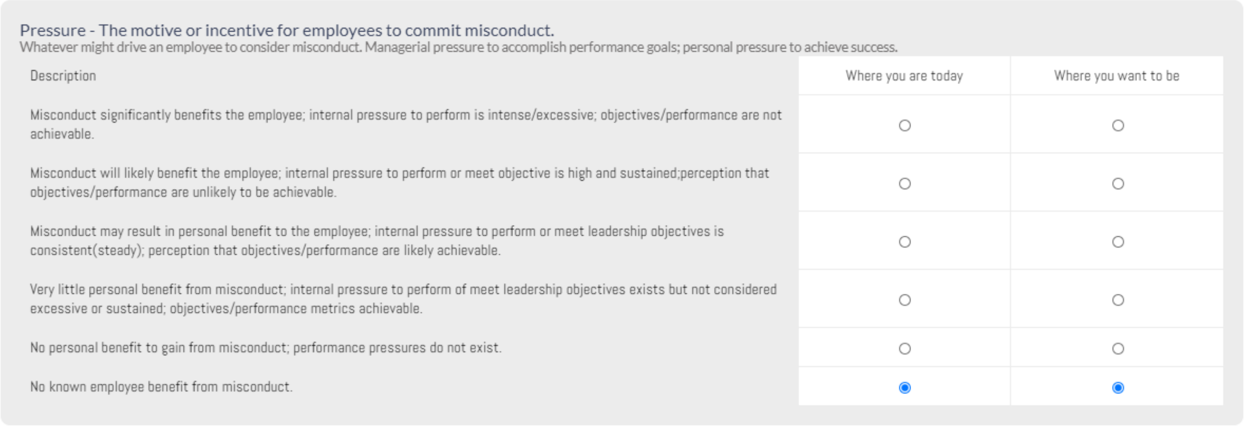


Opportunity - The ease with which an employee can commit misconduct
Also defined as - the means to execute whatever misconduct the employee has decided to do; effectiveness of compliance controls.

Description	Where you are today	Where you want to be
No known internal controls exist.	○	○
No automated controls; manual controls exist, but have not been audited or are audited infrequently; potential to override exists with no known method of detection.	○	○
Majority of controls are manual in nature, some automation exists to detect misconduct, some history of detection in the past; potential to override controls exists; suspect to audit findings.	○	○
Majority of controls are manual in nature, some automation exists to detect misconduct; demonstrated identification; routinely audited; undetected override of controls in unlikely.	○	○
Automated and manual internal controls sufficient to prevent misconduct; demonstrated prevention; routinely audited; limited access to override controls.	○	○
Controls could be and should be automated and currently demonstrate effectiveness in detection and prevention.	●	●

Pressure

The motive or incentive for employees to commit misconduct. Whatever might drive an employee to consider misconduct. Managerial pressure to accomplish performance goals; personal pressure to achieve success.

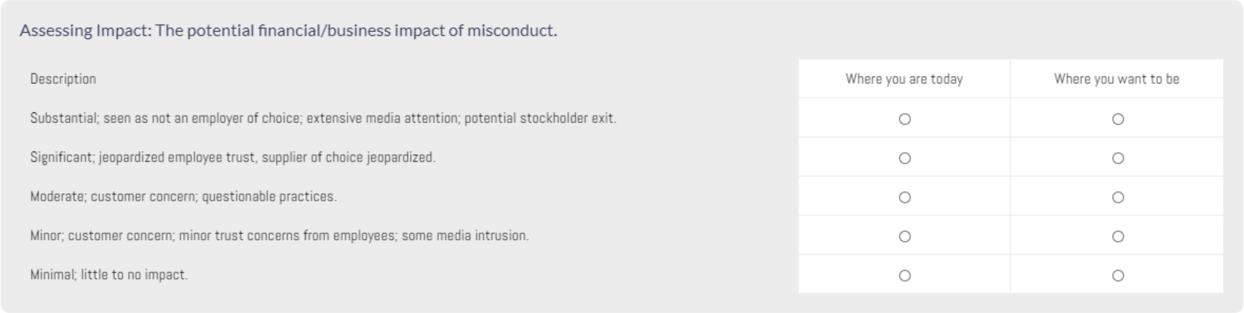


Pressure - The motive or incentive for employees to commit misconduct.
Whatever might drive an employee to consider misconduct. Managerial pressure to accomplish performance goals; personal pressure to achieve success.

Description	Where you are today	Where you want to be
Misconduct significantly benefits the employee; internal pressure to perform is intense/excessive; objectives/performance are not achievable.	○	○
Misconduct will likely benefit the employee; internal pressure to perform or meet objective is high and sustained;perception that objectives/performance are unlikely to be achievable.	○	○
Misconduct may result in personal benefit to the employee; internal pressure to perform or meet leadership objectives is consistent(steady); perception that objectives/performance are likely achievable.	○	○
Very little personal benefit from misconduct; internal pressure to perform of meet leadership objectives exists but not considered excessive or sustained; objectives/performance metrics achievable.	○	○
No personal benefit to gain from misconduct; performance pressures do not exist.	○	○
No known employee benefit from misconduct.	●	●

Consequence

Assessing Impact: The potential financial/business impact of misconduct.

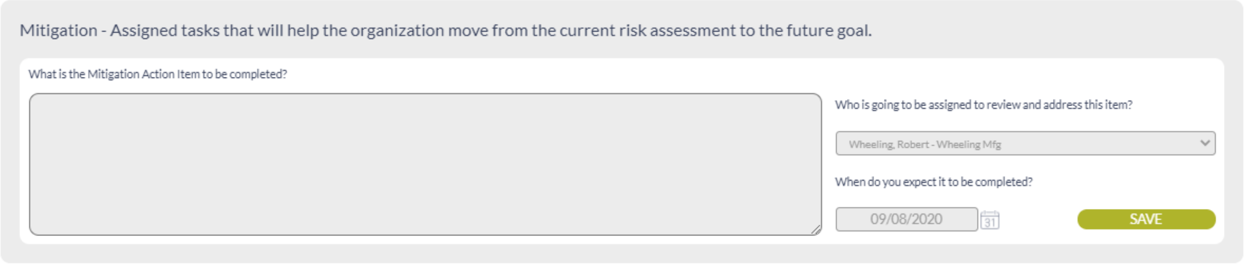


Assessing Impact: The potential financial/business impact of misconduct.

Description	Where you are today	Where you want to be
Substantial; seen as not an employer of choice; extensive media attention; potential stockholder exit.	○	○
Significant; jeopardized employee trust, supplier of choice jeopardized.	○	○
Moderate; customer concern; questionable practices.	○	○
Minor; customer concern; minor trust concerns from employees; some media intrusion.	○	○
Minimal; little to no impact.	○	○

Mitigation

Assigned tasks that will help the organization move from the current risk assessment to the future goal.



Mitigation - Assigned tasks that will help the organization move from the current risk assessment to the future goal.

What is the Mitigation Action Item to be completed?

Who is going to be assigned to review and address this item?

Wheeling, Robert - Wheeling Mfg

When do you expect it to be completed?

09/08/2020

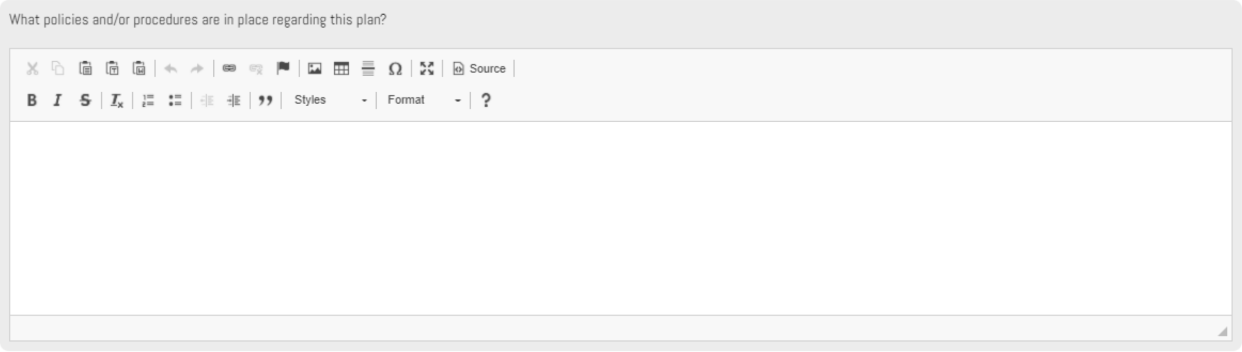
Assign a Mitigation Task by entering the details of the task to be completed, assign a user, select a due date and select Save. The task will be shown on the home page task list for the user assigned. The user will also receive an email notification of the task assignment.

Procedures

Your Procedures describe the "How" aspect of your compliance program. What internal documents are going to guide the management of this Plan? How are you going to communicate the rules and guidelines for managing the plan? What are the legal requirements you need to be aware of for this plan?

Policies & Procedures

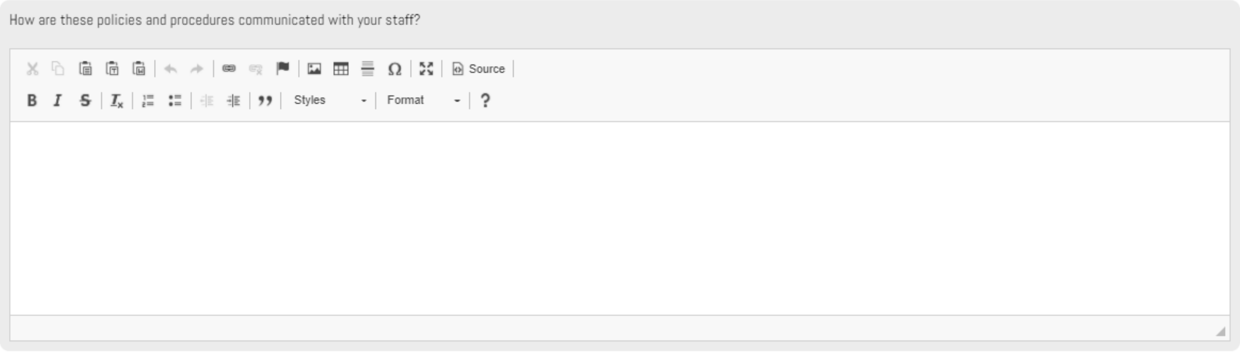
Enter the applicable policies and procedures related to the plan.



What policies and/or procedures are in place regarding this plan?

Communication

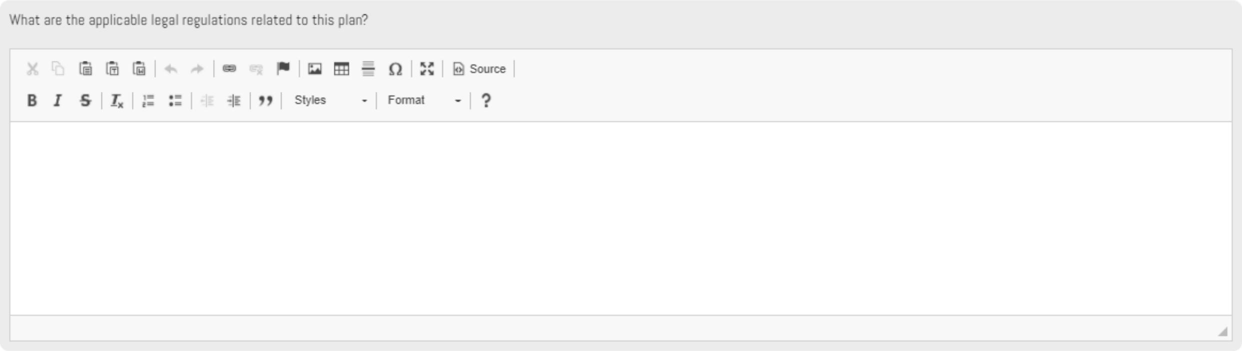
How are these policies and procedures communicated with your staff?



How are these policies and procedures communicated with your staff?

Legal Requirements

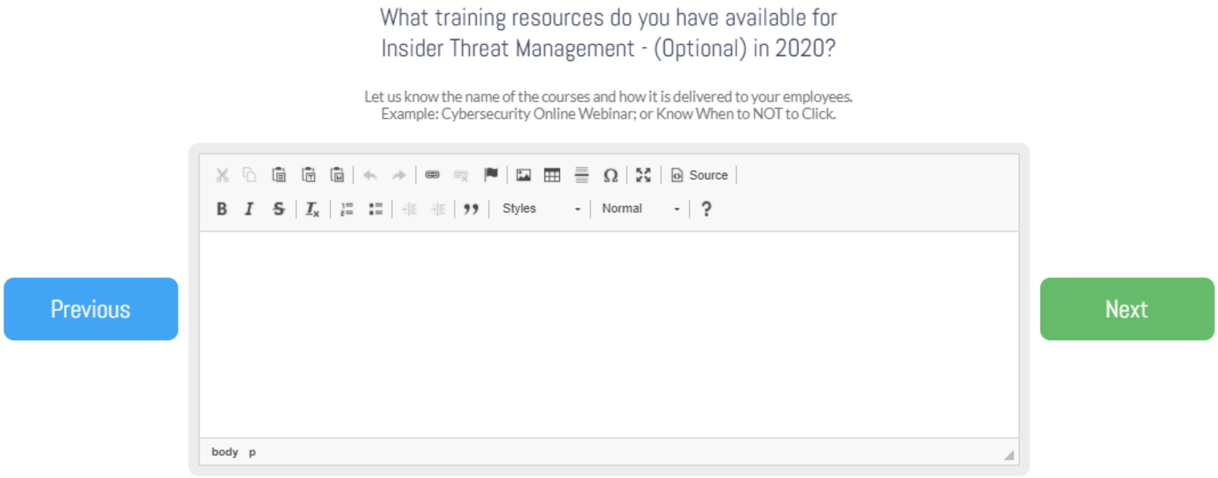
What are the applicable legal regulations related to this plan?



What are the applicable legal regulations related to this plan?

Training Plan

What training resources do you have available for Insider Threat Management? Let us know the name of the courses and how it is delivered to your employees. Example: Cybersecurity Online Webinar; or Know When to NOT to Click.

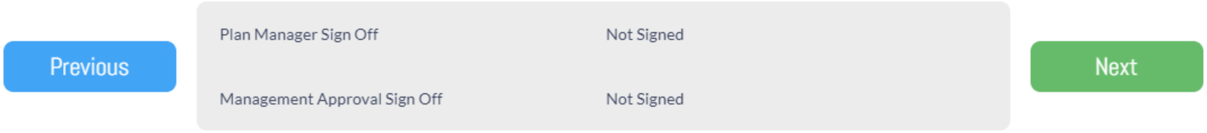


What training resources do you have available for Insider Threat Management - (Optional) in 2020?

Let us know the name of the courses and how it is delivered to your employees. Example: Cybersecurity Online Webinar; or Know When to NOT to Click.

Approval

Signature of the individuals responsible for approving the content of this compliance plan.



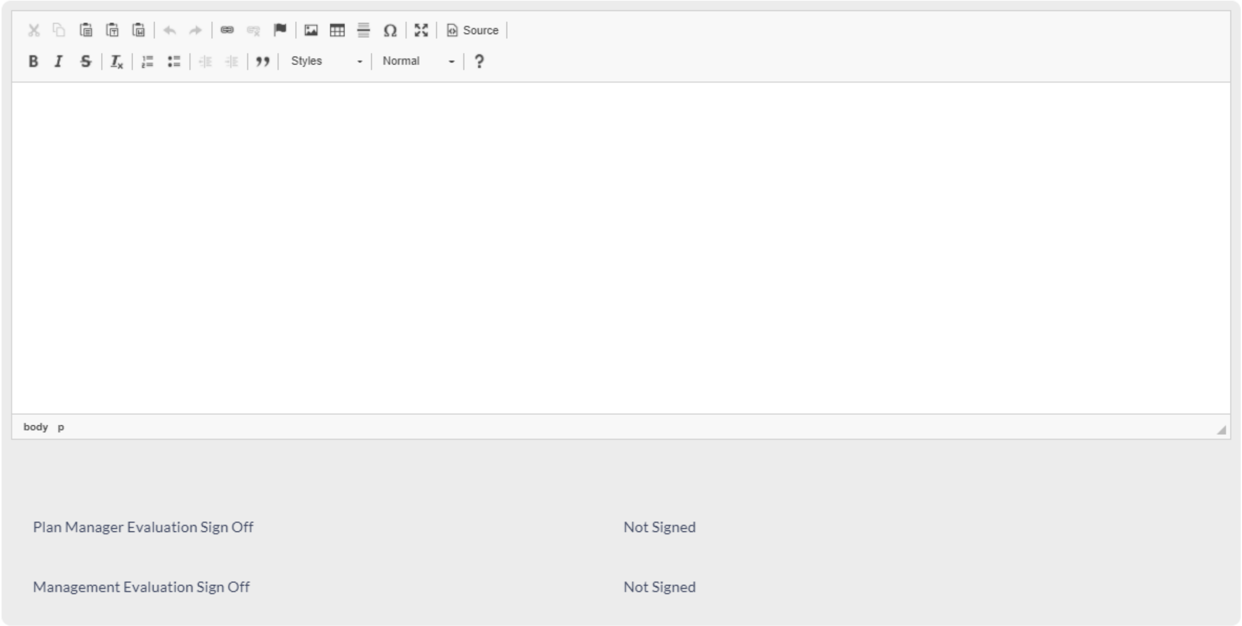
Plan Manager Sign Off	Not Signed
Management Approval Sign Off	Not Signed

The ability to sign off will only be enabled for the users selected in the Stakeholders tab.

Evaluation

Complete a year-end evaluation

- Identify and discuss any awareness activities performed during the year.
- Were any internal/external evaluations performed during the review period?
- Identify and discuss any changes to regulations that occurred during the plan year.
- Identify and discuss any changes to business activities/operations (relative to this plan) that occurred during the plan year.
- Identify and discuss any plan activity that will not complete during the year and why.



Plan Manager Evaluation Sign Off	Not Signed
Management Evaluation Sign Off	Not Signed

Signatures will only be enabled when the users assigned in Stakeholders are accessing this section.

Click the Complete button to return to the Certification Assistant Premium home page.